



Infosec incidents

- practical incident management
- computer forensics

Peeter Tatter

Infosec incidents

- Situation, when Something:
 - ☐ .. does not work quite well
 - ☐ .. is missing
 - ☐ .. too much of it (lines in logfile)
 - ☐ ..



First steps after identifying incident

- First step – what it is about

Organizational steps

- ☐ Who is qualified to decide, what to do?
 - ☐ Is there The Action Plan?
 - ☐ Who is involved and who should be involved?
- Can the incident end with police investigation?



Analysis of the initial information

■ Important first questions:

- ☐ When, who, what noticed?
- ☐ What has been done already and what has happened after that?
- ☐ How to obtain more detailed information?
- ☐ What to do next?
- ☐ How to manage information?

Restoring services vs preserving evidence

■ How to restore services ASAP?

- ☐ Use backup system, leave compromised system for analysis
- ☐ Restore system to new media, leave media of the compromised system for later analysis
- ☐ .. or .. let's try to restore services somehow and'll worry other things later (cost efficient, we „had“ a backup)



Collecting information, sources

- computers
- logs
 - servers
 - firewalls
 - Access and security systems
- Security camera recordings
- People
- Backup copies



Storing and transporting collected data

- With computers:

- ☐ Store the PC/server
- ☐ Store media
- ☐ Make copy of the media
- ☐ Copy only files

- logfiles

- ☐ Do not filter – or – preserve as much as possible
- ☐ cryptohash everything



Analysing data inside the computer

IMPORTANT! Avoid altering data.

Traditional approach:

- Do not power on
- Do not use running computer, remove power (battery from laptop)
- What was connected and where ... ?
- Disconnect peripherals, take computer and go ...



Basic rules

Avoid using the original system

- ☐ Never run the system from original media
- ☐ Remove and duplicate media
- ☐ Sometimes you may run computer from live-cd

Rule – store original data and work on the copy



Copying the data for analysis

preferred:

- *cloning*
- *disk imaging*

- *volume imaging*
- *logical imaging*
- *copying*



Copying

Checking the authenticity

- ☐ Checksum clone, image (MD5/SHA1)
- ☐ Checksum smaller data blocks (CRC)
- ☐ Checksum files

Copying ...

Formats

- dd (*raw image*)
 - ☐ Most universal
 - ☐ No automatic checksumming
- E0x
 - ☐ *de facto* (EnCase) /some years ago .../
 - ☐ Automatic checksumming (MD5, CRC)
 - ☐ Includes image metadata describing media
 - ☐ Closed data format :-)



Copying ...

Selecting OS:

- ☐ Linux
- ☐ Live CD-d (Helix)
- ☐ Something special

Copying ...

Forensic disc duplicators:

- Portable independent device
- Cloning and duplicating
- Speed <4GB/min
- Checksumming during cloning
- Automatic logging

Commonly used devices:

- Logicube MD5/Talon/Quest
- Tableau TD1
- ImageMASSter Solo



After copying ...

What's next?

- Checksum both – original and clone - NOW!
- Write down date/time of the computer
- Make backup of the cloned/copied data

Now, let's analyze ...



Analyzing

■ Interpreting filesystems

- FAT12, FAT16, FAT32

- NTFS

- EXT2/EXT3, Reiser

- HFS/HFS+

- FFS/UFS/UFS2

- ISO9660/Joliet/UDF



Analyzing

■ Restoring erased files:

- ☐ Data is erased when it is overwritten
- ☐ Interpreting file descriptors of deleted files on filesystem level
- ☐ ...
- ☐ No miracles if information has been overwritten
- ☐ SSD “problems” can help, mostly fixed



Analyzing

- Space unused by the filesystem
 - Unused clusters
 - Physical and logical size of the file (*file slack*)
 - Unpartitioned space

This space can be filled with data, how to find it?



Analyzing

Keyword search

- ☐ Realtime search
- ☐ Indexed search
- ☐ regexp-search

- different encodings (ä, ц, や)



Analyzing

- Preview of file contents
- Picture gallery
- Using file type signature database
- Checksum comparison
- (semi)automatic documenting, summaries ...



Tools

Historical:

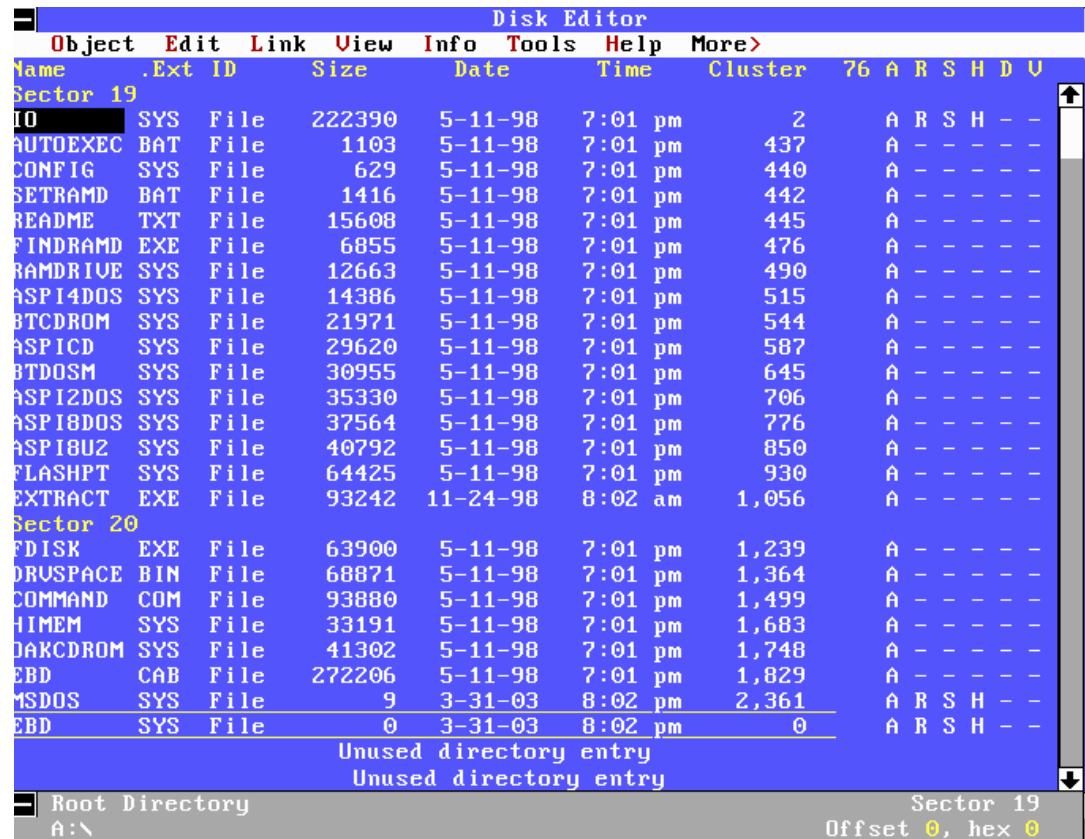
- Norton Disk Edit (diskedit.exe)
- TCT - The Coroners Toolkit

Current:

- TSK (The Sleuth Kit)
 - Autopsy
 - PTK
- EnCase
- FTK (Forensic Toolkit)
- X-Ways Forensics (WinHex)

Tools - Norton Disk Edit

- One of the first
- Is not specialised
- Can interpret only FAT-filesystem
- Mostly used as a learning tool
- Lot's of forks and developments based on it



The screenshot shows the Norton Disk Editor interface. At the top is a menu bar with 'Object', 'Edit', 'Link', 'View', 'Info', 'Tools', 'Help', and 'More'. Below the menu is a table of files. The table has columns for Name, .Ext, ID, Size, Date, Time, Cluster, and a set of flags (76 A R S H D U). The files are listed in two sections: Sector 19 and Sector 20. The files include IO, AUTOEXEC, CONFIG, SETRAMD, README, FINDRAMD, RAMDRIVE, ASPI4DOS, BTCDROM, ASPICD, BTDOSM, ASPI2DOS, ASPI8DOS, ASPI8U2, FLASHPT, EXTRACT, FDISK, DRUSPACE, COMMAND, HIMEM, DAKCDROM, EBD, MSDOS, and another EBD. The bottom of the window shows 'Root Directory A:\' and 'Sector 19 Offset 0, hex 0'.

Name	.Ext	ID	Size	Date	Time	Cluster	76	A	R	S	H	D	U
Sector 19													
IO	SYS	File	222390	5-11-98	7:01 pm	2	A	R	S	H	-	-	
AUTOEXEC	BAT	File	1103	5-11-98	7:01 pm	437	A	-	-	-	-	-	
CONFIG	SYS	File	629	5-11-98	7:01 pm	440	A	-	-	-	-	-	
SETRAMD	BAT	File	1416	5-11-98	7:01 pm	442	A	-	-	-	-	-	
README	TXT	File	15608	5-11-98	7:01 pm	445	A	-	-	-	-	-	
FINDRAMD	EXE	File	6855	5-11-98	7:01 pm	476	A	-	-	-	-	-	
RAMDRIVE	SYS	File	12663	5-11-98	7:01 pm	490	A	-	-	-	-	-	
ASPI4DOS	SYS	File	14386	5-11-98	7:01 pm	515	A	-	-	-	-	-	
BTCDROM	SYS	File	21971	5-11-98	7:01 pm	544	A	-	-	-	-	-	
ASPICD	SYS	File	29620	5-11-98	7:01 pm	587	A	-	-	-	-	-	
BTDOSM	SYS	File	30955	5-11-98	7:01 pm	645	A	-	-	-	-	-	
ASPI2DOS	SYS	File	35330	5-11-98	7:01 pm	706	A	-	-	-	-	-	
ASPI8DOS	SYS	File	37564	5-11-98	7:01 pm	776	A	-	-	-	-	-	
ASPI8U2	SYS	File	40792	5-11-98	7:01 pm	850	A	-	-	-	-	-	
FLASHPT	SYS	File	64425	5-11-98	7:01 pm	930	A	-	-	-	-	-	
EXTRACT	EXE	File	93242	11-24-98	8:02 am	1,056	A	-	-	-	-	-	
Sector 20													
FDISK	EXE	File	63900	5-11-98	7:01 pm	1,239	A	-	-	-	-	-	
DRUSPACE	BIN	File	68871	5-11-98	7:01 pm	1,364	A	-	-	-	-	-	
COMMAND	COM	File	93880	5-11-98	7:01 pm	1,499	A	-	-	-	-	-	
HIMEM	SYS	File	33191	5-11-98	7:01 pm	1,683	A	-	-	-	-	-	
DAKCDROM	SYS	File	41302	5-11-98	7:01 pm	1,748	A	-	-	-	-	-	
EBD	CAB	File	272206	5-11-98	7:01 pm	1,829	A	-	-	-	-	-	
MSDOS	SYS	File	9	3-31-03	8:02 pm	2,361	A	R	S	H	-	-	
EBD	SYS	File	0	3-31-03	8:02 pm	0	A	R	S	H	-	-	
Unused directory entry													
Unused directory entry													
Root Directory A:\													
												Sector 19	
												Offset 0, hex 0	

Tools - TCT

The Coroners Toolkit

- Presented 1991,
D. Farmer ja W. Vienema
- Minly for analyzing
Unix'es
- Collection of CLI tools,
Perl ja C
- Free
(IBM Public Licence)

<http://www.porcupine.org/forensics/tct.html>



René Magritte "La trahison des images"



Tools - TSK

The Sleuth Kit

- Collection of CLI tools
- Improved TCT
- Supports: Linux, OS X, FreeBSD, OpenBSD, and Solaris
- Recognizes FAT, NTFS, UFS, EXT2FS, and EXT3FS
- Free (CPL, IBM Public License)

<http://www.sleuthkit.org/sleuthkit/>



Tools – Autopsy ja PTK

GUI for TSK

- Autopsy – created by TSK team
- PTK – alternative by DFLabs

<http://www.sleuthkit.org/autopsy/>

<http://ptk.dflabs.com/>



Tools - EnCase

- MS Windows based tool
- Very common, *de facto* standard
- Intuitive and user friendly GUI
- Modular design
- Good end user support and active community
- Closed source commercial software, quite expensive



Tools - FTK

- MS Windows based
- Second most popular
- User friendly, less technical than EnCase, less options
- Powerful indexing search engine
- Some filesystems are supported
- Closed source commercial software



Tools – comparison

- CLI tools may be problematic when analyzing big case. Requires self discipline.
- Using GUI tools may end with random „surfing“
- Best tools are really, really expensive
- There is no universal tool!



„Traditional forensics“ vs „live forensics“

Traditional forensics

- Avoid tampering original data

Live forensics

- Avoid tampering original data and store data in the memory



Analyzing powered on computer

Additional data from powered-on computer:

- ☐ Active processes and data about them
- ☐ Information about network connections
- ☐ Mounted external disks, crypto containers
- ☐ Other data in the RAM

How to store all this and avoid tampering data on the media?



Analyzing powered on computer

Manually

- ☐ Applications, processes, network connections ...
- ☐ Mounted media, copy of mounted media ...
- ☐ ...
- ☐ Power off, and back to step one (copy media ...)

Avoid, if possible ...



Analyzing working computer

Tools for dumping memory:

- psinfo/pslist/psfile/psloggedon (SysInternals)
- PMDump/MemImager (Arne Vidstrom)
- mdd (SourceForge)
- winen (EnCase pakettis)



Analyzing working computer

Tools for automated analysis:

- WFT (Windows Forensic Toolchest)
- COFEE (Computer Online Forensic Evidence Extractor) /by Microsoft/



Finally

- Leave it to professionals
- Be prepared for the worst (as a potential victim)
- If you are targeted, try to preserve as much evidence as possible
- Time factor ...